Republic of the Philippines
Office of the Solicitor General
134 Amorsolo St., Legaspi Village, Makati City

Technical Working Group for
Information and Communications Technology

TERMS OF REFERENCE

SUBSCRIPTION TO FILE AND DATA BACKUP SOLUTION

Background:

The Office of the Solicitor General (OSG) represents the government in legal matters, provides legal advice, and oversees critical legal functions that demand secure and efficient data management. In the digital age, the OSG relies heavily on online productivity platforms, especially cloud-based solutions like Microsoft O365, to collaborate, store, and manage essential case files and legal documentation. These platforms host vast amounts of sensitive and confidential information crucial for legal operations, necessitating the implementation of robust data management protocols. The risks posed by data loss—whether due to accidental deletion, system failures, cyberattacks, or natural disasters—could severely disrupt legal processes and compromise the integrity of governmental legal work. Therefore, safeguarding this data ensures continuous access to essential legal resources.

To mitigate these risks, the OSG has identified the need for a comprehensive data backup and restoration solution that integrates with its existing Microsoft O365 environment. Such a solution would provide automated, reliable backups of files, emails, calendars, and other productivity data, ensuring that all mission-critical information can be swiftly recovered during data loss. By providing consistent cloud data backup, the OSG aims to enhance its operational resilience and maintain the continuity of legal services under all circumstances.

Objective:

The proposed backup and data restoration solution ensures that the Office of the Solicitor General can securely store and retrieve its Microsoft O365 cloud-based files, emails, and productivity data. This solution will enable regular automated backups, providing the OSG with reliable access to critical information, even in the event of accidental deletions, data corruption, or cyber threats such as ransomware. The focus will be on creating a seamless backup system that integrates with the OSG's existing infrastructure and allows authorized personnel to efficiently restore data when required, minimizing downtime and disruptions to ongoing legal processes.

In addition, the solution aims to comply with stringent legal and security requirements, ensuring the confidentiality, integrity, and availability of sensitive government data. The OSG can manage data backups, monitor restoration processes, and maintain detailed audit trails for all backup and recovery activities by implementing a user-friendly interface with advanced security controls. The

overarching goal is to safeguard the OSG's digital assets while providing the legal team with uninterrupted access to vital information.

Terms:

1. *Scope.* – Subscription to File and Data Backup Solution

2. *ABC.* - The Approved Budget for the Contract (ABC) is **Four Million Pesos (₱4,000,000.00)**, including all government taxes, charges, and other standard fees.

ICT SUBSCRIPTION			
ITEM	**QTY**	**UNIT COST**	**TOTAL**
SUBSCRIPTION TO FILE AND DATA BACKUP SOLUTION (850 Units)	1	4,000,000.00	4,000,000.00
		TOTAL	**₱ 4,000,000.00**

3. *Schedule of Payment.* - To guarantee the performance by the winning bidder of its obligations under the contract, it shall post a performance security before the signing of the contract. The performance security shall be in an amount not less than the required percentage of the total contract price in any of the following forms and in accordance with the following schedule:

Form of Performance Security	Amount of Performance Security (Not less than the required % of the Total Contract Price)	Statement of Compliance
a) Cash or cashier's/ manager's check issued by a Universal of Commercial Bank.	5%	
b) Bank draft/ guarantee or irrevocable letter of credit issued by a Universal or Commercial Bank; *however,* it shall be confirmed or authenticated by a Universal or Commercial Bank if issued by a foreign bank.	5%	
c) Surety bond callable upon demand issued by a surety or insurance company duly certified by the Insurance Commission as authorized to issue such security.	30%	

TERMS OF PAYMENT	Statement of Compliance
Supplier agrees to be paid based on a progressive billing scheme as follows:	
• Within thirty (30) days from completion of the delivery and issuance of the Inspection and Acceptance Report by the OSG and submission of all other required documents - 95% of the contract price. • One (1) year from the issuance of the Inspection and Acceptance Report by the OSG - 5% of the contract price.	

All bid prices shall be considered as fixed prices and, therefore, not subject to price escalation during contract implementation.

4. *Qualifications of the Supplier*:

   a. The bidder must have completed, within the last three years from the submission date and receipt of at least one (1) single contract of a similar nature amounting to at least fifty percent (50%) of the ABC.

      The definition of a similar contract is the provision of file and data backup for the cloud.

   b. The bidder shall submit a valid and current Certificate of Distributorship/Dealership/ Resellers of the product being offered, issued by the principal or manufacturer of the product (if the bidder is not the manufacturer). If not issued by the manufacturer, must also submit a certification/document linking the bidder to the manufacturer.

   c. During contract implementation, the bidder/supplier must remain an authorized distributor, reseller, or partner to maintain said License Software. Suppose the bidder/supplier cannot maintain its distributor, reseller, or partnership agreement with the Manufacturer/Principal. In that case, this may serve as a ground for terminating its contract with OSG.

   d. The bidder must have at least one (1) certified engineer who can support the solution.

   e. The financial proposal shall include all costs necessary for the supplier to fulfill its obligation to deliver and deploy the file and data backup solution (software, hardware, etc.).

5. *Delivery and Training*:

a. All items should be delivered within 30 days of receipt of the Notice to Proceed or before anniversary date of existing contract whichever comes first.
b. .

a. Provide training covering essential items for correct use and day-to-day administration.

b. Training materials, product guides, and documentation should be available online.

c. Must be done during business hours

d. The course outline should be presented.

e. Training must begin upon deployment within ten (10) days of solution delivery and must be coordinated with CMS. The CMS will provide certification for delivery and training completion.

6. Applicable provisions of the Government Procurement Reform Act (RA No. 9184 and RA No. 12009) and its Revised Implementing Rules and Regulations (RIRR) shall form part of the Terms of Reference.

Technical Specifications:

ITEM	SPECIFICATIONS	COMPLIANCE
1. GENERAL		
1.1	– The solution must be a backup service providing comprehensive data protection and data recovery for Microsoft Exchange, SharePoint, OneDrive for Business, and Teams, giving the OSG complete control of its Microsoft 365 environment.	
1.2	– The solution shall allow configuration to grant access to restore selected Exchange Online and OneDrive accounts based on AD security groups.	
1.3	– The solution shall save information about backup and restore sessions, where you can review this information in a log.	
1.4	– The solution shall support email notifications about backup and restore job results.	
1.5	– The solution must be capable of generating the following reports: Mailbox Protection Report, User Protection Report, Backup Summary Report, Restore Activity Report, and Backup Policy Detail Report.	
1.6	– The solution shall use modern app-only authentication when you add Microsoft 365 organizations	
1.7	– The solution shall support the backup of Microsoft Teams channel messages using Microsoft Teams APIs in Microsoft Graph (Teams Export APIs).	
1.8	– The solution shall include a built-in storage facility in the Asia Pacific region.	
1.9	– The data must be encrypted: • During transition, when the solution is performing backup and restoration activities. • When the data is at rest at the solution's storage facility.	
1.10	– The solution shall back up all Office 365 data for all active, licensed users of the OSG.	
1.11	– The solution shall retain all Office 365 backup data for the retention period to meet the retention policy defined.	

1.12	– The solution shall support exit from SaaS to a customer-hosted model gracefully at any point of the contract term.	
1.13	– After the exit, the solution shall be able to continue incremental backups without requiring full backups. Existing restore points should also remain based on the retention policy configured.	
1.14	– The solution shall provide a portal that is a web-based solution that allows the administrator to perform the following: • Backup configuration and monitoring • Restoration of backed-up data.	
1.15	– The cost for data transfer and storage for the backup data shall be included in the license.	
2. BACKUP DATA		
2.1	– The solution shall be able to define a list of users, groups, sites, teams, and organizations to back up and a schedule according to which new backups must be created.	
2.2	– The solution shall allow customer to specify object types and their processing and exclusion options when creating and configuring backup jobs. The following object types are available for backup and restore: • Organizations • Groups • Users • Sites • Teams	
2.3	– Backup job shall run automatically in accordance with the schedule.	
2.4	– The customer shall be able to define and configure: • Backup frequency • Retention policy	
2.5	– The solution must automatically resume interrupted search jobs during planned maintenance.	
2.6	– The solution shall deliver the appropriate level of protection to different data sets by setting up multiple backup policies with different schedules.	

2.7	– The solution shall allow end users to choose to opt some organization users for lightning-quick backups and quick (bulk) restore operations.	
3. RESTORE DATA		
3.1	– The solution shall allow the restoration of backup data for Office 365 Services at a file or folder level.	
3.2	– The solution shall allow restoring or exporting backup data for Office 365 Services to alternate locations, local computers, or in place.	
3.3	– The solution shall allow restoration and export of Exchange Online data from backups from point-in-time restores, either at the mailbox, folder, or item level.	
3.4	– The solution shall compare data with the Exchange Online to track differences in your backups.	
3.5	– The solution shall allow the restoration and export of SharePoint Online data and metadata, including backup permissions.	
3.6	– The solution must be capable of restoring personal SharePoint sites to a different location within the same tenant.	
3.7	– The solution shall allow restoration of OneDrive data from backups.	
3.8	– The solution shall allow the restoration and export of Microsoft Teams data from backups to Teams Chats, Teams Channel, and Teams Calendar.	
3.9	– The solution shall be able to recover with minimal downtime and effort when you recover multiple Microsoft 365 users in a single operation.	
4. DATA RETENTION - MICROSOFT BACKUP STORAGE (MBS)		
4.1	– The solution shall utilize Microsoft Backup Storage, wherein all backup data is stored within the organization's Microsoft 365 tenant.	
4.2	– The data retention period is governed by the Microsoft 365 Backup Storage policies, which typically support retention from 14 days up to 1 year	

5. BACKUP INTERVAL (RPO) FOR MICROSOFT BACKUP STORAGE (MBS)		
5.1	– The backup intervals for the Express Edition are aligned with Microsoft 365 Backup Storage capabilities.	
5.2	– Exchange, OneDrive, and SharePoint must support frequent backups, with RPO as low as every 10 minutes or less, depending on Microsoft's configuration and service tier.	
6. OTHER REQUIREMENTS/FUNCTIONALITIES		
6.1	– The solution shall be an All-inclusive backup service with **unlimited storage**.	
6.2	– The solution includes service-level immutability capabilities on the primary backup, at no additional cost to the customer, based on how the data is protected.	
6.3	– Licensing is based on the number of M365 user accounts and not on capacity.	
6.4	– The solution should have regular penetration tests carried out by a 3rd party specialist provider.	
6.5	– The solution offers advanced security capabilities, including granular Role-Based Access Control.	
6.6	– The solution must have a search mechanism that allows users to find items matching specified search criteria	
6.7	– The solution must have the ability to perform granular, file-level recoveries and self-service options.	
6.8	– The solution uses Local Redundant Storage (LRS) by default, where 3 copies of customer data are stored on 3 separate disks within the primary region.	
6.9	– The solution utilizes Microsoft single sign-on with Multi-Factor Authentication.	
6.10	– The solution must offer a 99.9% uptime SLA, excluding planned outages.	
6.11	– The solution must have the ability to monitor backup data, receive alerts on changes, and generate reports for compliance purposes.	

6.12	– The solution must have the ability to separate backup data from production, and change the infrastructure location	
7. IMPLEMENTATION SERVICES		
5.1	– Perform the onboarding procedure of Data Cloud for Microsoft 365	
5.2	– Configure a backup repository to store the backup data.	
5.3	– Create a backup job based on the required backup policy.	
5.4	– Configure user and role on the Data Cloud for Microsoft 3653	
5.5	– Perform backup of Exchange, SharePoint OneDrive, and Teams	
5.6	– Verify that the backup job is running successfully.	
5.7	– Create and provide As-built Documentation	
5.8	– Provide knowledge transfer	
8. CERTIFICATIONS		
8.1	– The Bidder must have a certified engineer	
8.2	– The Solution should be a Leader in Gartner Magic Quadrant Enterprise Backup and Recovery Software Solutions for at least 8th consecutive years and positioned highest in Ability to Execute (a certification from the vendor must be submitted as part of the technical requirements)	
9. MAINTENANCE SUPPORT		
	For support and services, the bidder must have the following:	
6.1	– Unlimited corrective maintenance/ repair services within the warranty period	
6.2	– Twenty-four (24) hours by seven (7) days (Monday to Sunday) technical support, and must meet the following response and resolution time: ▪ Critical incidents <30 minutes ▪ Critical threats <60 minutes ▪ Root cause analysis for all support cases filed.	
6.3	– The bidder must provide full documentation for the Activity Plan on	

	installing patches and upgrades, and Root Cause Analysis of incidents encountered.	
6.4	– The bidder must provide on-site support for installing and deploying software patches and version upgrades.	
6.5	– The bidder must provide a procedure for support and problem escalation	
6.6	– Submission of Activity/Service Report within 5 calendar days after rendering service	
6.7	– The bidder must conduct system health checks every quarter with the following scope: ▪ System/Application patches, fixes, security patches, and alerts ▪ System/Application profile ▪ Resource utilization ▪ Log analysis ▪ Formal reports on the output of conducted health checks within 5 days	

Technical Working Group for ICT Subscriptions

SSS JOEL N. VILLASERAN

DIR IV EDUARDO ALEJANDRO O. SANTOS

SSII OMAR T. GABRIELES

ITO III JAYVIE NEIL MALICK S. MALICDEM

ITO II CEDRIC S. DELA CRUZ

CMT III JESUS NIÑO CHUA

AO IV RAY CHARLIE V. ALEGRE

Approved/Disapproved:

DARLENE MARIE B. BERBERABE
Solicitor General

Certified Funds Available:
UNDER NEP 2026

ASG SAMANTHA P. CAMITAN
OIC - FMS